ECE 498KL: eCrime and Internet Service Abuse

Ransomware

Kirill Levchenko

December 6, 2018

ILLINOIS

Electrical & Computer Engineering

COLLEGE OF ENGINEERING

Monetizing Installs

- Fake antivirus software
- **Ransomware**
- Spam bots
- Information theft
- Cryptocurrency mining
- Adware
- Freemium software

Ransomware

- What is *ransomware?*

  Malware that encrypts files on a victim's computer and demands ransom in exchange for decryption.

- Ransoms range from $200—$2,000

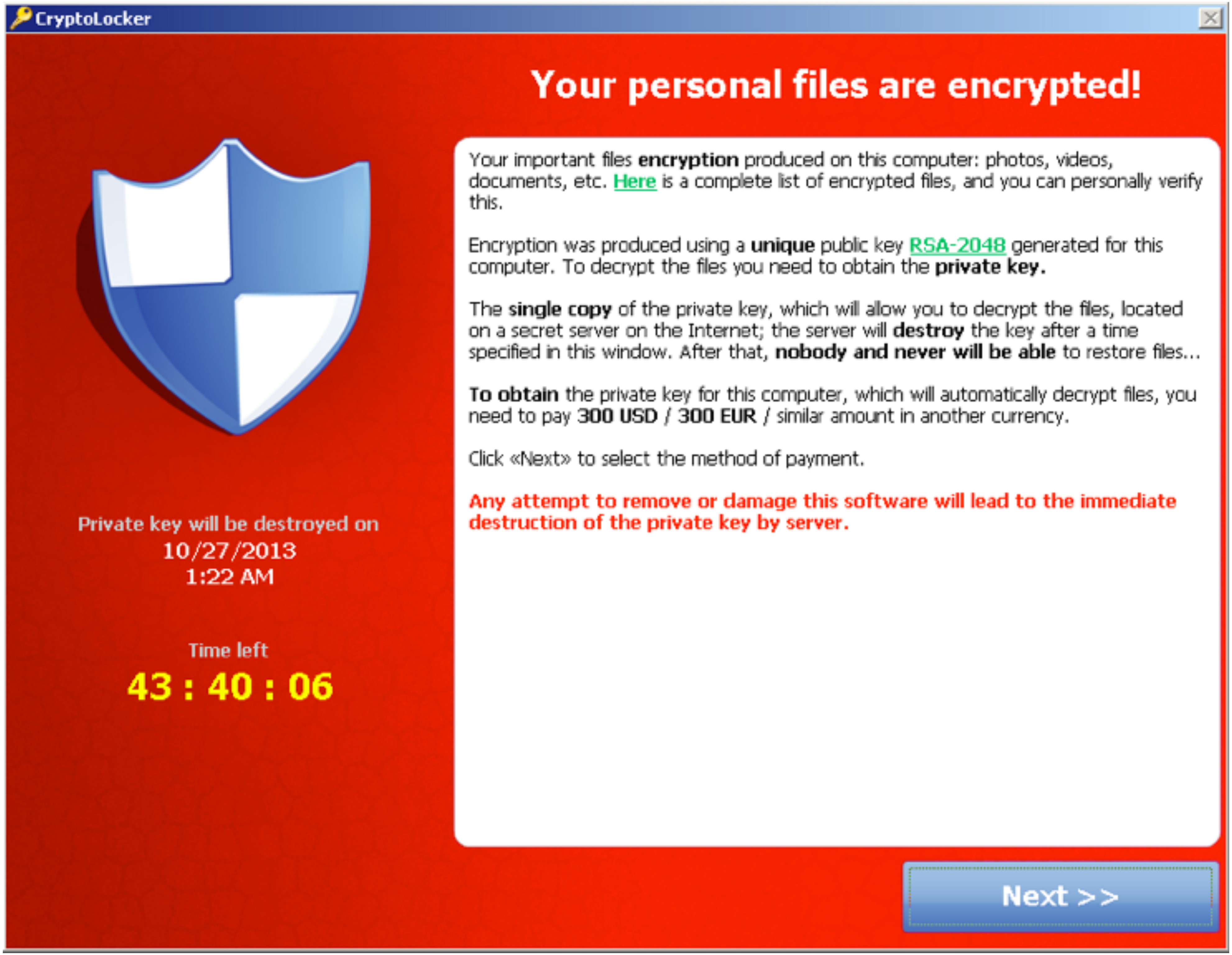
- Payment often via Bitcoin

- Ransom often honored with decryption key

Cryptolocker

- First major ransomware (2013)
  - Spread via an email purporting to come from UPS or FedEx
- Demanded $300 in ransom
  - 41% paid according to University of Kent
  - 3% paid according to Symantec
  - 0.4% paid according to Dell SecureWorks

    100×
  - Estimated revenue of $27M



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

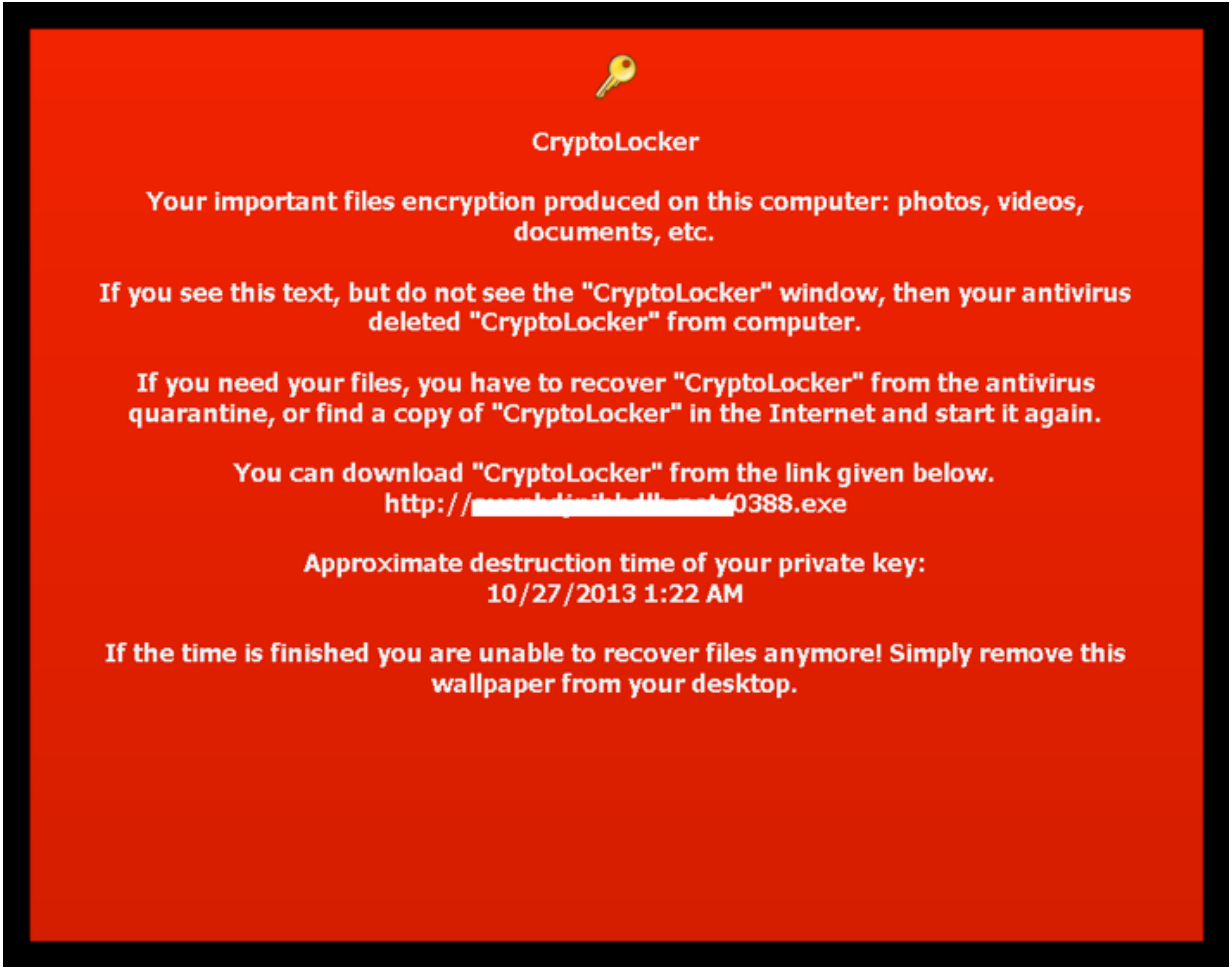
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/27/2013
1:22 AM

Time left
43 : 40 : 06



CryptoLocker

Your important files encryption produced on this computer: photos, videos, documents, etc.

If you see this text, but do not see the "CryptoLocker" window, then your antivirus deleted "CryptoLocker" from computer.

If you need your files, you have to recover "CryptoLocker" from the antivirus quarantine, or find a copy of "CryptoLocker" in the Internet and start it again.

You can download "CryptoLocker" from the link given below.
http://[redacted]0388.exe

Approximate destruction time of your private key:
10/27/2013 1:22 AM

If the time is finished you are unable to recover files anymore! Simply remove this wallpaper from your desktop.

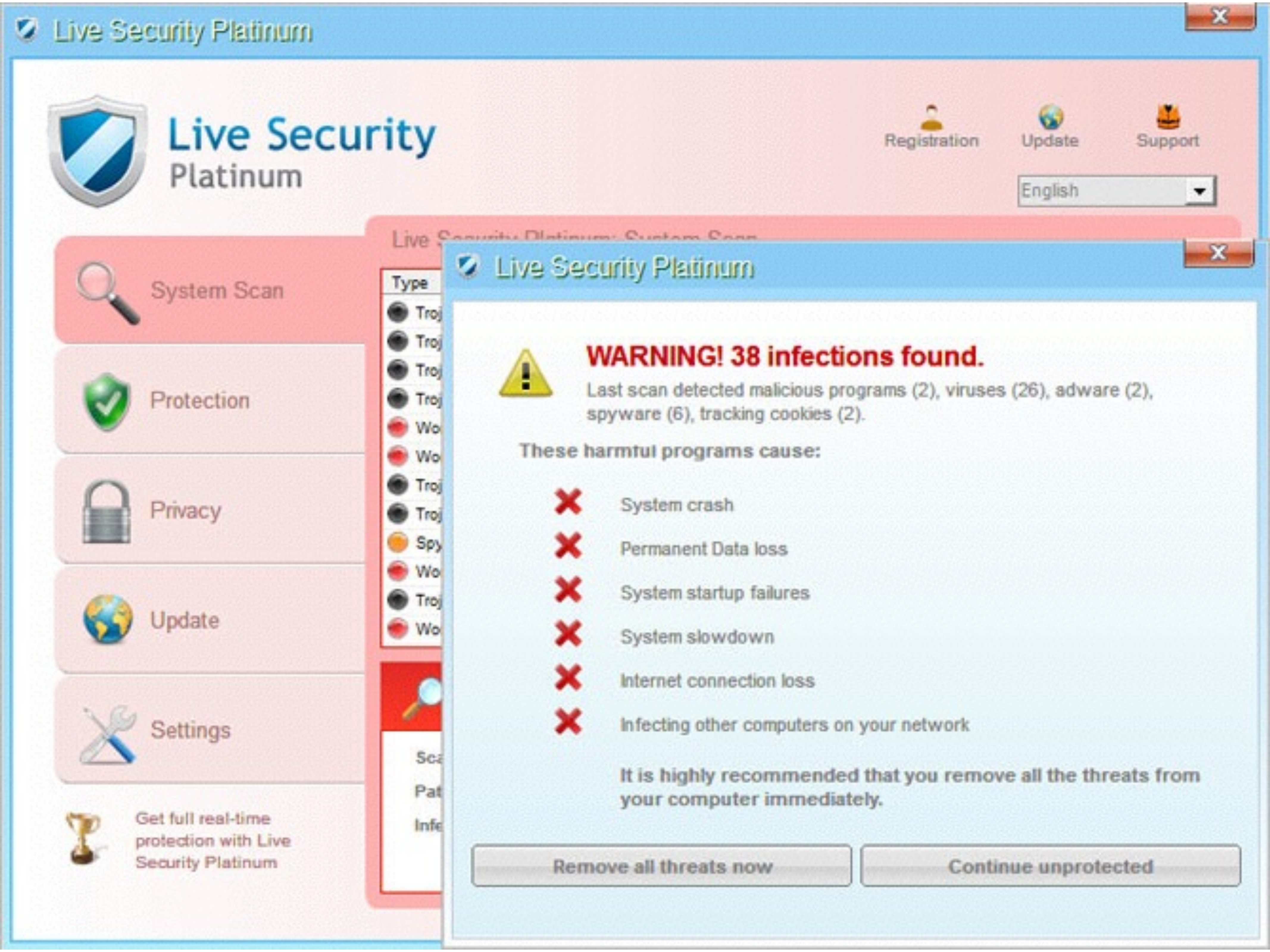
Evolution from FakeAV

FAKEAV variants typically scare users into doling out cash with fake alerts touting computer infection

Early ransomware variants scared users with screen lockouts

Today’s ransomware variants not only lock users out of their systems but also threaten to delete all of their files if they do not pay the ransom

source: Trend Micro. Ransomware: Past, Present, and Future, 2017.



WARNING! 38 infections found.

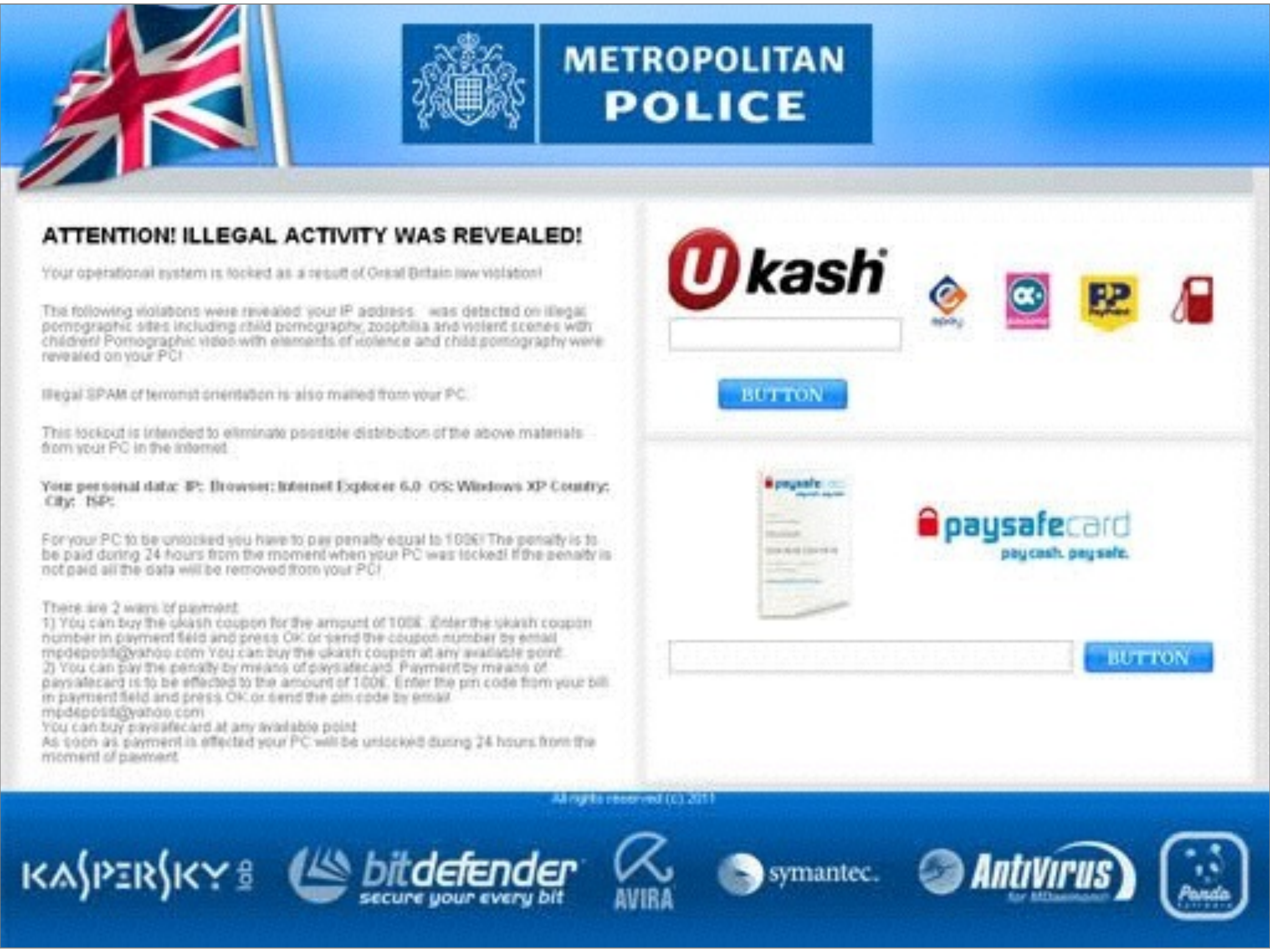
Last scan detected malicious programs (2), viruses (26), adware (2), spyware (6), tracking cookies (2).

These harmful programs cause:

- ✗ System crash
- ✗ Permanent Data loss
- ✗ System startup failures
- ✗ System slowdown
- ✗ Internet connection loss
- ✗ Infecting other computers on your network

It is highly recommended that you remove all the threats from your computer immediately.

Get full real-time protection with Live Security Platinum



ATTENTION! ILLEGAL ACTIVITY WAS REVEALED!

Your operational system is locked as a result of Great Britain law violation!

The following violations were revealed: your IP address was detected on illegal pornographic sites including child pornography, zoophilia and violent scenes with children! Pornographic video with elements of violence and child pornography were revealed on your PC!

Illegal SPAM of terrorist orientation is also mailed from your PC.

This lockout is intended to eliminate possible distribution of the above materials from your PC in the internet.

Your personal data: IP: Browser: Internet Explorer 6.0 OS: Windows XP Country: City: ISP:

For your PC to be unlocked you have to pay penalty equal to 100£! The penalty is to be paid during 24 hours from the moment when your PC was locked! If the penalty is not paid all the data will be removed from your PC!

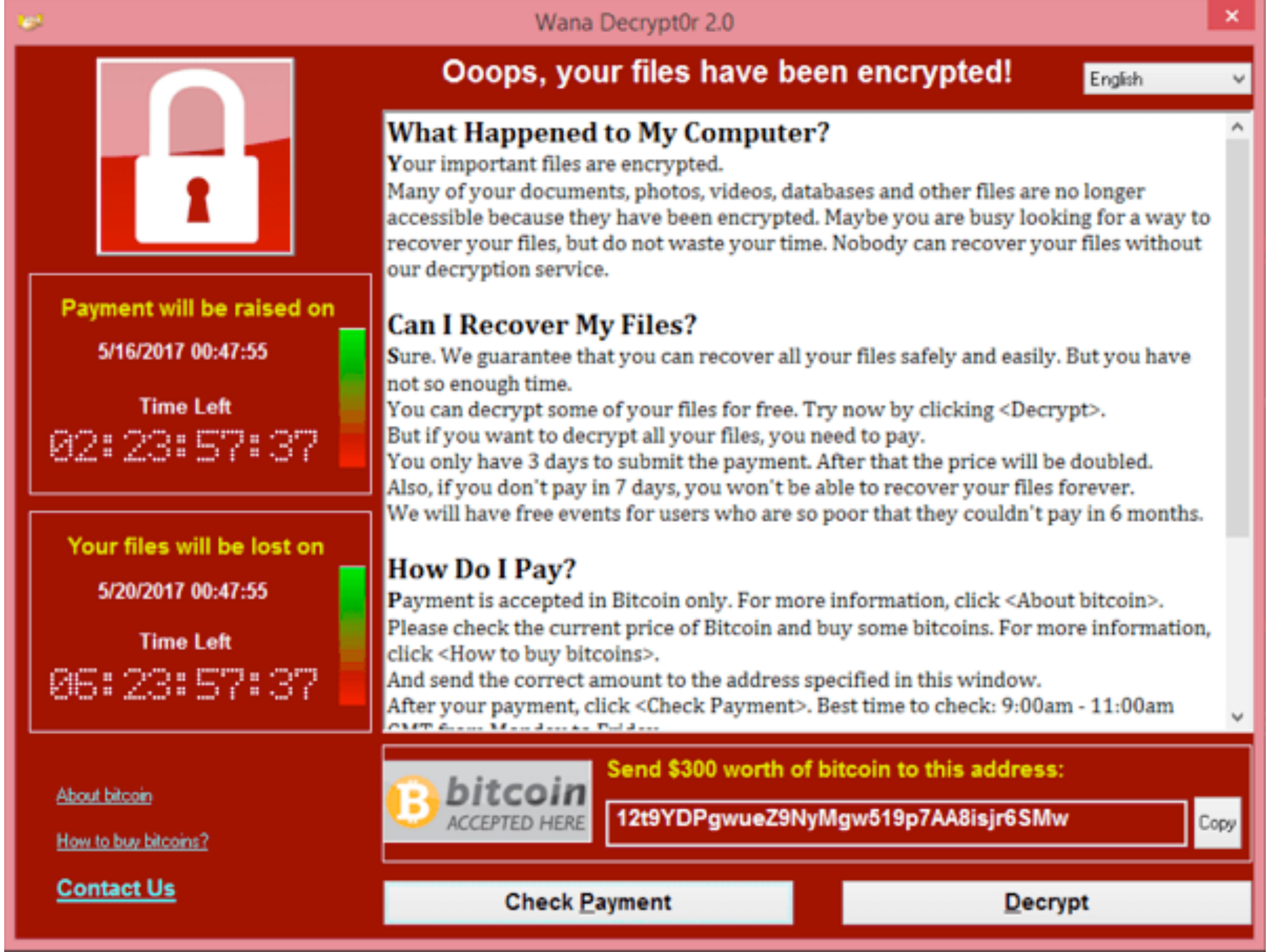
There are 2 ways of payment:
1) You can buy the ukash coupon for the amount of 100£. Enter the ukash coupon number in payment field and press OK or send the coupon number by email mpdeposit@yahoo.com You can buy the ukash coupon at any available point.
2) You can pay the penalty by means of paysafecard. Payment by means of paysafecard is to be effected to the amount of 100£. Enter the pin code from your bill in payment field and press OK or send the pin code by email mpdeposit@yahoo.com
You can buy paysafecard at any available point.
As soon as payment is effected your PC will be unlocked during 24 hours from the moment of payment.

All rights reserved (c) 2011

WannaCry

- On May 12, 2017, several organizations were affected by a new ransomware strain.
- The ransomware was very successful in part because it used a SMB vulnerability to spread inside networks.
- The vulnerability was patched by Microsoft in March for supported versions of Windows.
- The exploit, known under the name **ETERNALBLUE**, was released in April as part of a leak of NSA tools.

source: SANS. WannaCry/WannaCrypt Ransomware, 2017.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

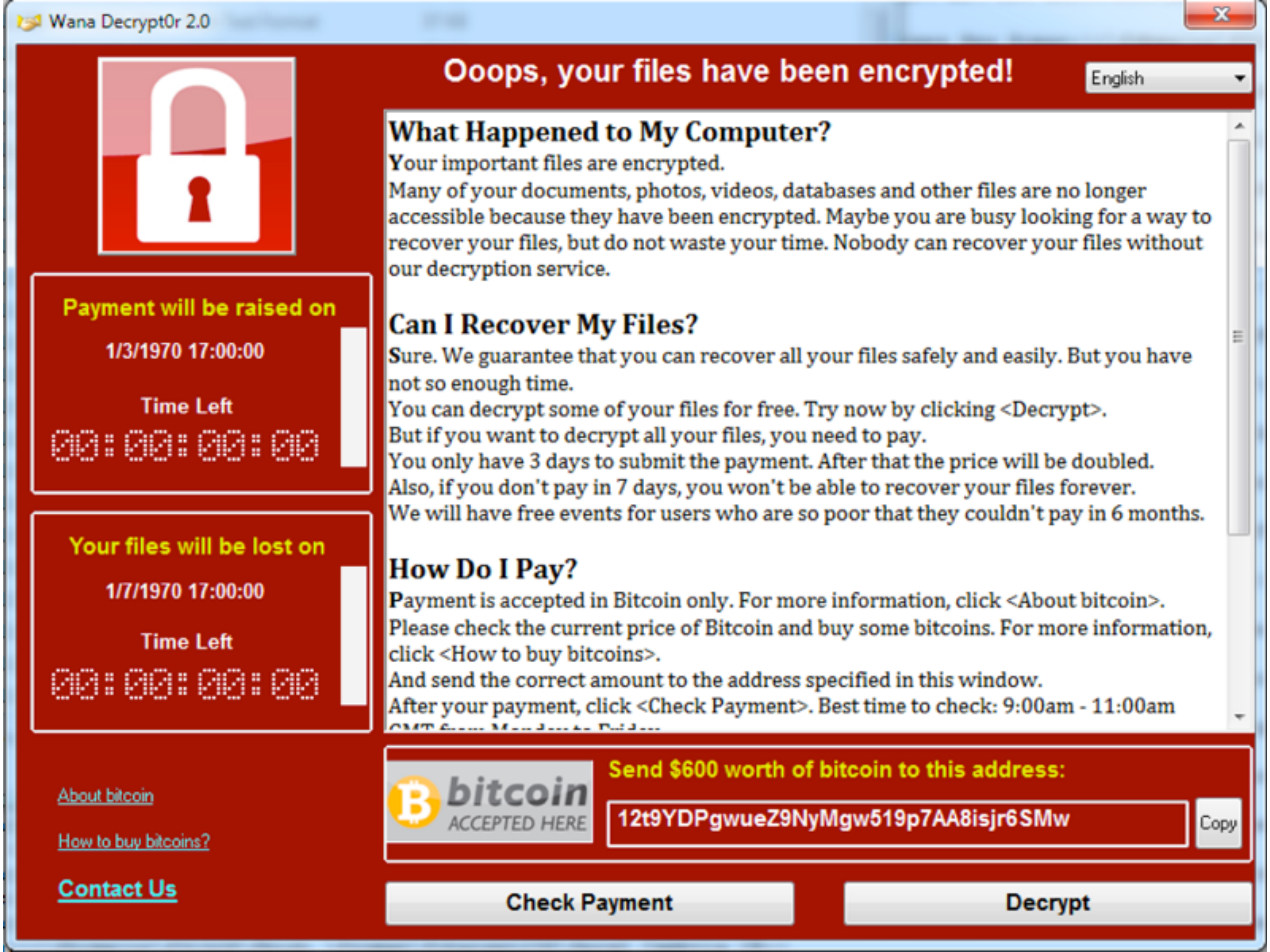
How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on

1/3/1970 17:00:00

Time Left

00:00:00:00

Your files will be lost on

1/7/1970 17:00:00

Time Left

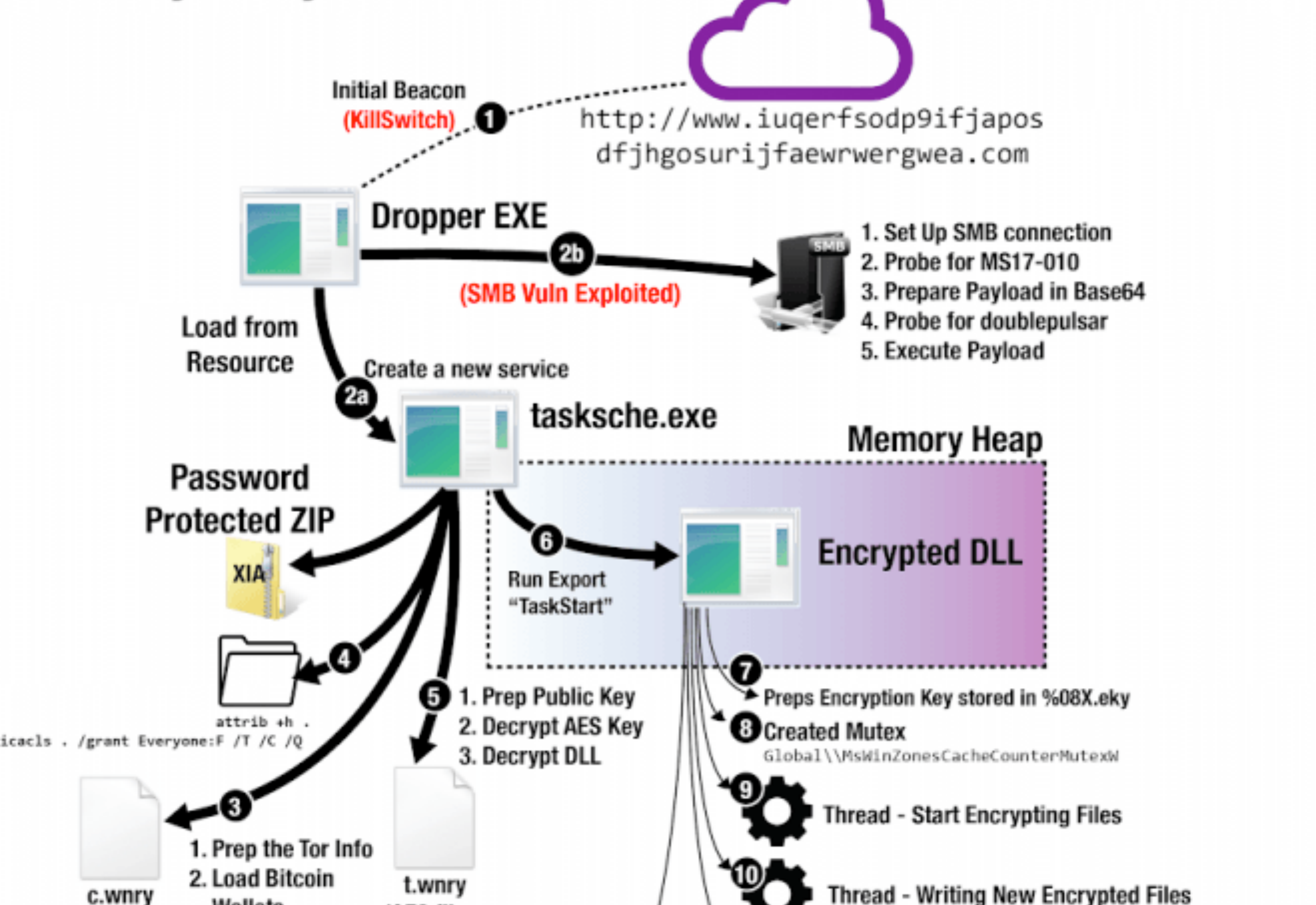
00:00:00:00

Send $600 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

WanaCry/WCry Execution Flow

ENDGAME.



Initial Beacon
(KillSwitch)
1
http://www.iuqerfsodp9ifjapos
dfjhgosurijfaewrwergwea.com

Dropper EXE

2b
(SMB Vuln Exploited)

1. Set Up SMB connection
2. Probe for MS17-010
3. Prepare Payload in Base64
4. Probe for doublepulsar
5. Execute Payload

Load from
Resource

2a
Create a new service

tasksche.exe

Memory Heap

Password
Protected ZIP

6
Run Export
"TaskStart"

Encrypted DLL

4
`attrib +h .`
`icacls . /grant Everyone:F /T /C /Q`

5
1. Prep Public Key
2. Decrypt AES Key
3. Decrypt DLL

7
Preps Encryption Key stored in %08X.eky

8
Created Mutex
`Global\\MsWinZonesCacheCounterMutexW`

3
1. Prep the Tor Info
2. Load Bitcoin
Wallets

c.wnry

t.wnry

9
Thread - Start Encrypting Files

10
Thread - Writing New Encrypted Files

WannaCry

- Used three fixed Bitcoin addresses to receive payment
    - 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
    - 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
    - 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- Attributed by some security companies to N. Korea
- Does *not* decrypt on payment

WannaCry Impact

“This attack reportedly infected 209,653 machines in 99 countries. Hospitals, universities, transport infrastructure, and cash dispensers have been the victims of this attack. FedEx in the United States, the British healthcare system NHS, and the Spanish operator Telefonica have all been affected. In France, the Renault plant in Sandouville was put out of operation in order to regain control of its production tools.”

Sébastien Gest. Jaff and Wannacry Ransomware Analysis, 2017.

WannaCry Impact

“The NHS responded well to what was an unprecedented incident, with no reports of harm to patients or of patient data being compromised or stolen. In total, 1% of NHS activity was directly affected by the WannaCry attack. 802 3 out of 236 hospital trusts across England were affected4, which means that services were impacted even if the organisation was not infected by the virus (for instance they took their email offline to reduce the risk of infection). 595 out of 7,4545 GP practices (8%) and eight other NHS and related organisations were infected. This disruption to patient care has made it even clearer how dependent the NHS is on information technology and, as a result, the need for security improvements to be made across the service.”

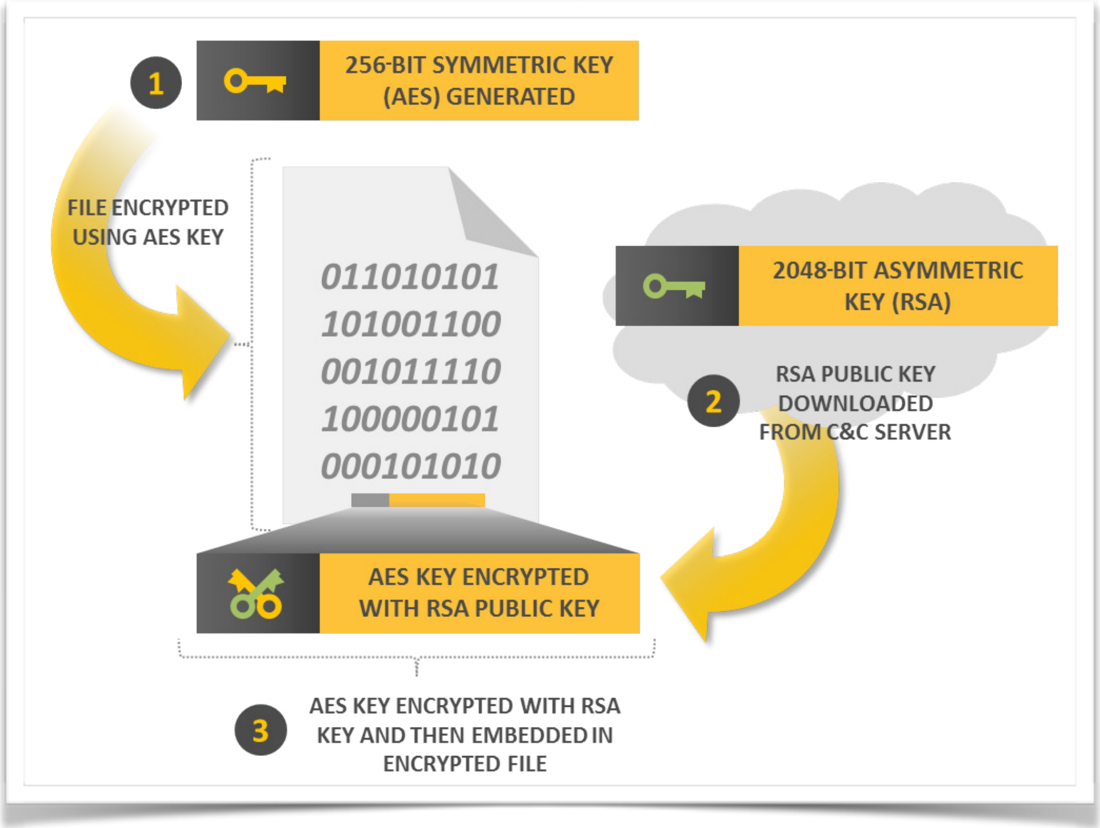
William Smart. Lessons learned review of the WannaCry Ransomware Cyber Attack, 2018.

Ransomware Workflow

- Contact command-and-control server
  - Get encryption public key
  - Get Bitcoin payment address
- Encrypt files
- Demand ransom
- Decrypt using private key provided when ransom paid

Crypto Variation A

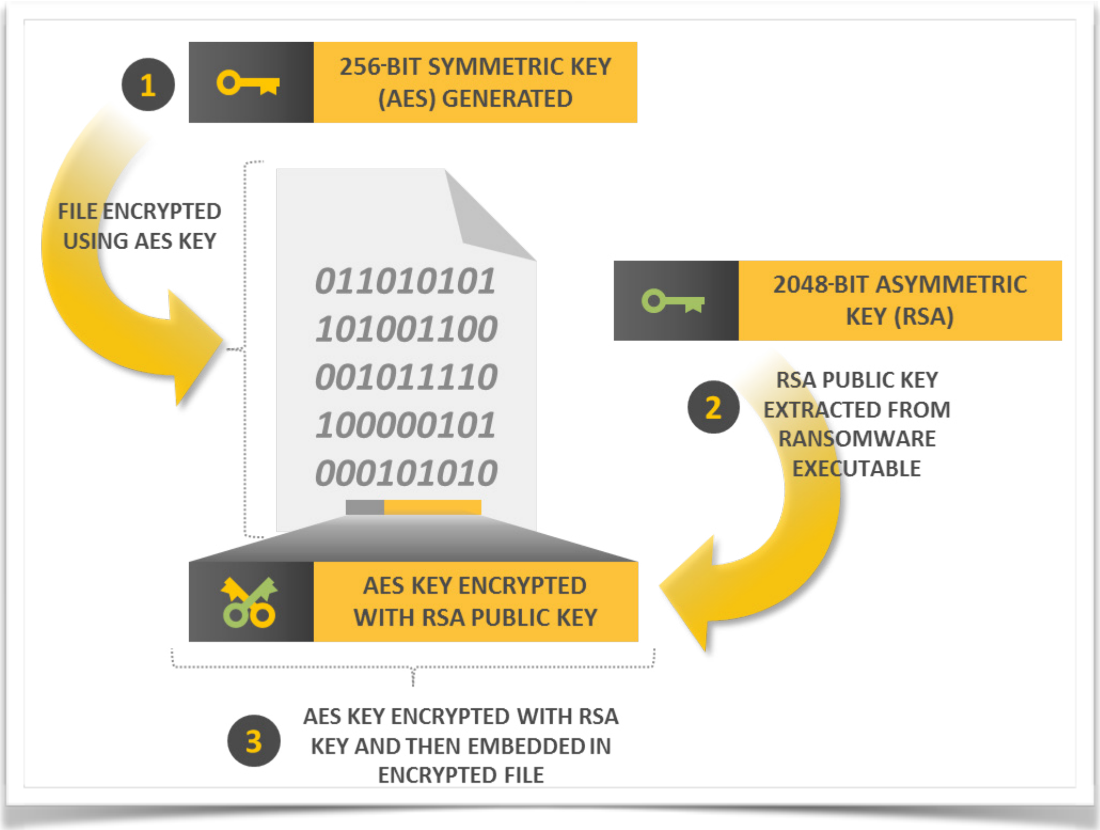
1. Generate symmetric key and encrypt files
2. Get a public key from server
3. Encrypt symmetric key using public key and append to file


1
256-BIT SYMMETRIC KEY (AES) GENERATED
FILE ENCRYPTED USING AES KEY
011010101
101001100
001011110
100000101
000101010
2048-BIT ASYMMETRIC KEY (RSA)
2
RSA PUBLIC KEY DOWNLOADED FROM C&C SERVER
AES KEY ENCRYPTED WITH RSA PUBLIC KEY
3
AES KEY ENCRYPTED WITH RSA KEY AND THEN EMBEDDED IN ENCRYPTED FILE

source: k. Savage *et al.* The evolution of ransomware, 2015.

Crypto Variation B

1. Generate symmetric key and encrypt files
2. Use public key hard-coded into executable
3. Encrypt symmetric key using public key and append to file



1 256-BIT SYMMETRIC KEY (AES) GENERATED

FILE ENCRYPTED USING AES KEY

011010101
101001100
001011110
100000101
000101010

2048-BIT ASYMMETRIC KEY (RSA)

2 RSA PUBLIC KEY EXTRACTED FROM RANSOMWARE EXECUTABLE

AES KEY ENCRYPTED WITH RSA PUBLIC KEY

3 AES KEY ENCRYPTED WITH RSA KEY AND THEN EMBEDDED IN ENCRYPTED FILE

source: k. Savage *et al.* The evolution of ransomware, 2015.

Ransomware	Crackable?	Details
2.1 Apocalypse	Crackable	Weak algorithm
2.2 Cerber	Was crackable, currently not	The second-level key used to be leaked by its C&C server.
2.3 CryptoWall	Non-crackable	It cannot run because C&C server is down.
2.4 CTB_Locker	Non-crackable	None
2.5 Jigsaw	Crackable	Decryption key can be found in the ransomware sample.
2.6 Locky	Non-crackable	It cannot run because C&C server is down.
2.7 Petya	Crackable	The second-level key can be found, because the cryptographic
2.8 TeslaCrypt	Crackable	The ransomware author releases the first-level key (master key).
2.9 TorrentLocker	Non-crackable	None
2.10 Unlock92	Non-crackable	None

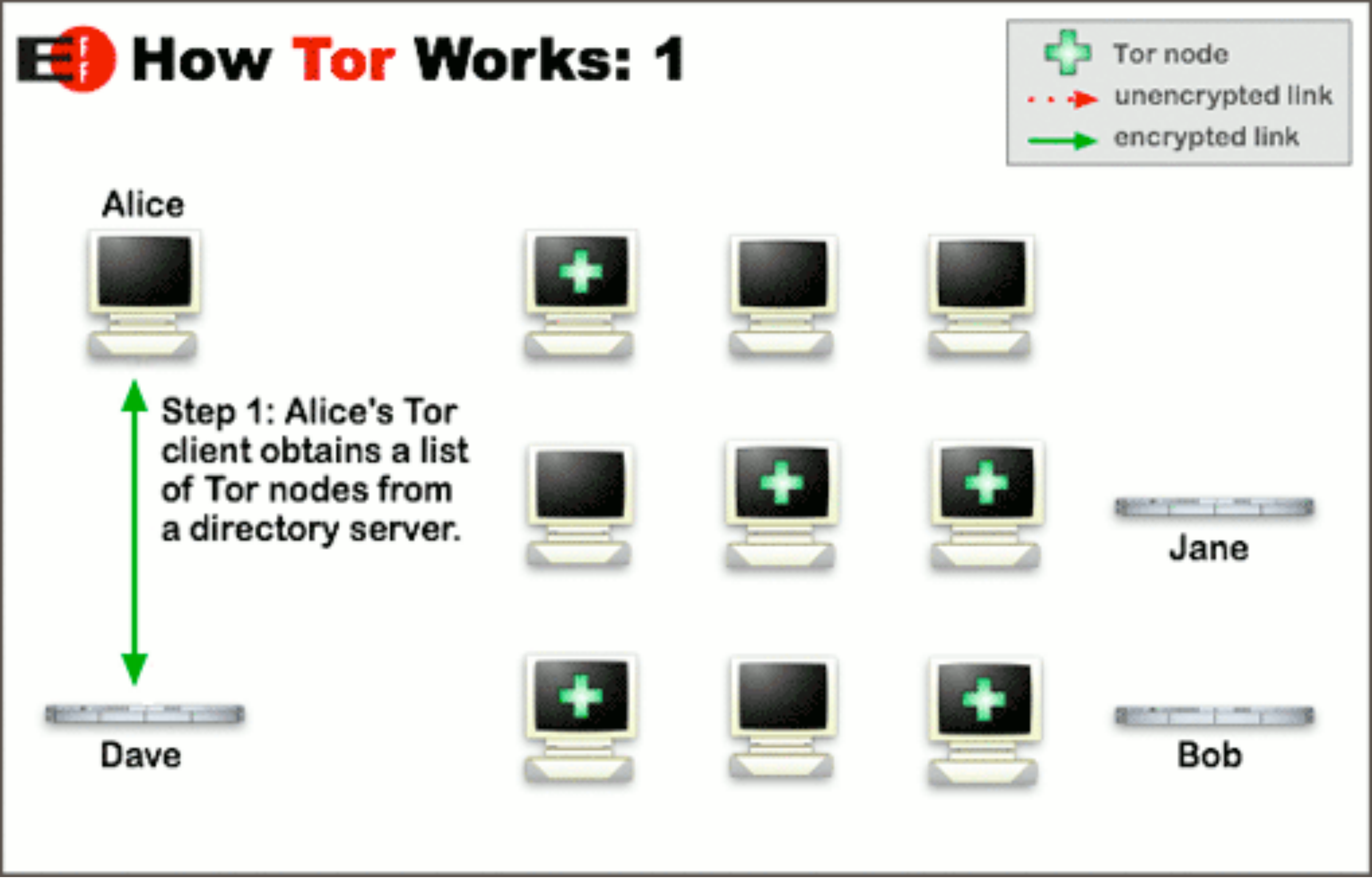
source: Yimi Hu. A Brief Summary of Encryption Method Used in Widespread Ransomware, 2017.

Ransom Payment

- Payment/support site uses Tor hidden services. Why?
  - Anonymity
  - Hard to shut down

Tor

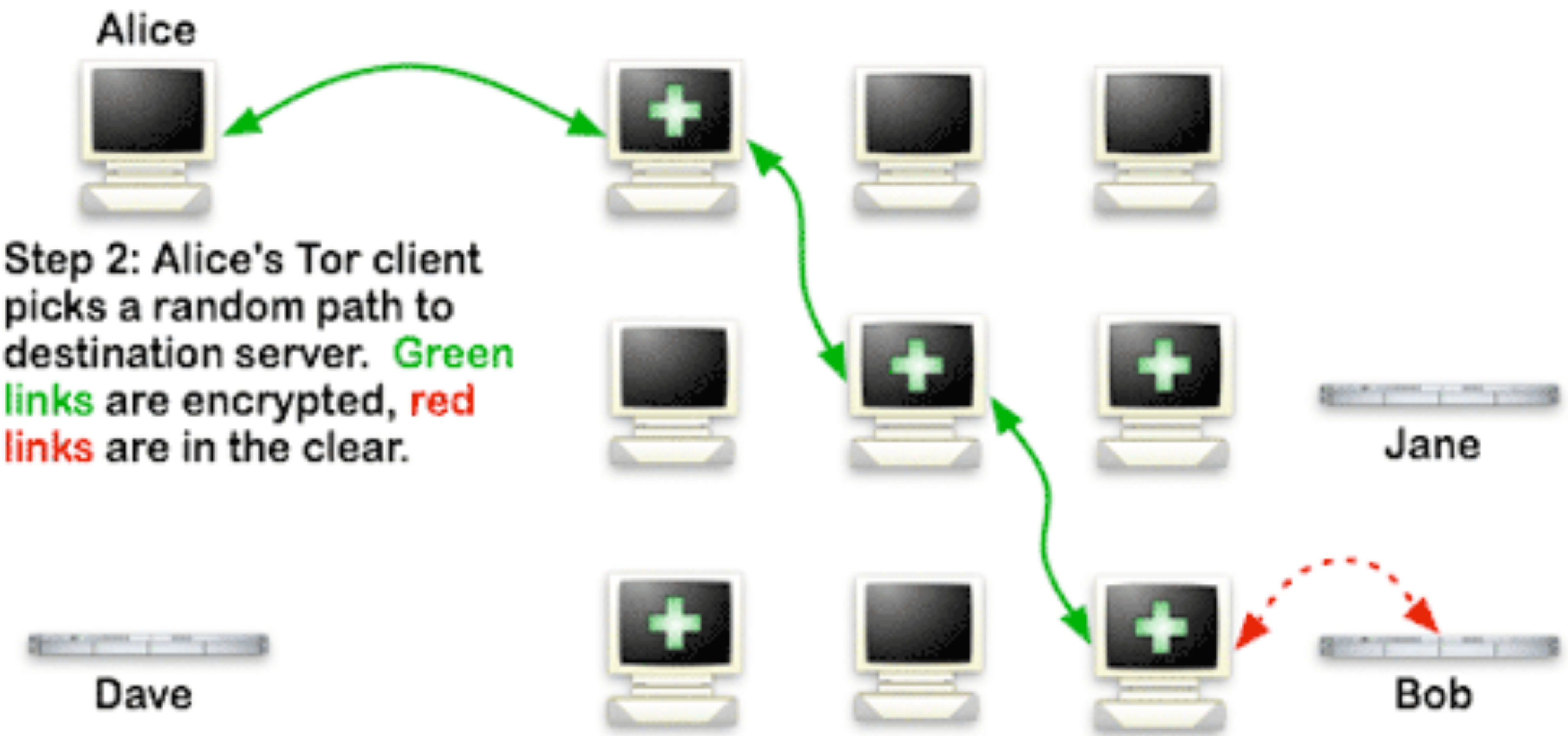
- Provides anonymity to Internet users
  - No one (except session initiator) knows who is communicating
  - Most common use: Web browsing



How Tor Works: 1

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.

How Tor Works: 2

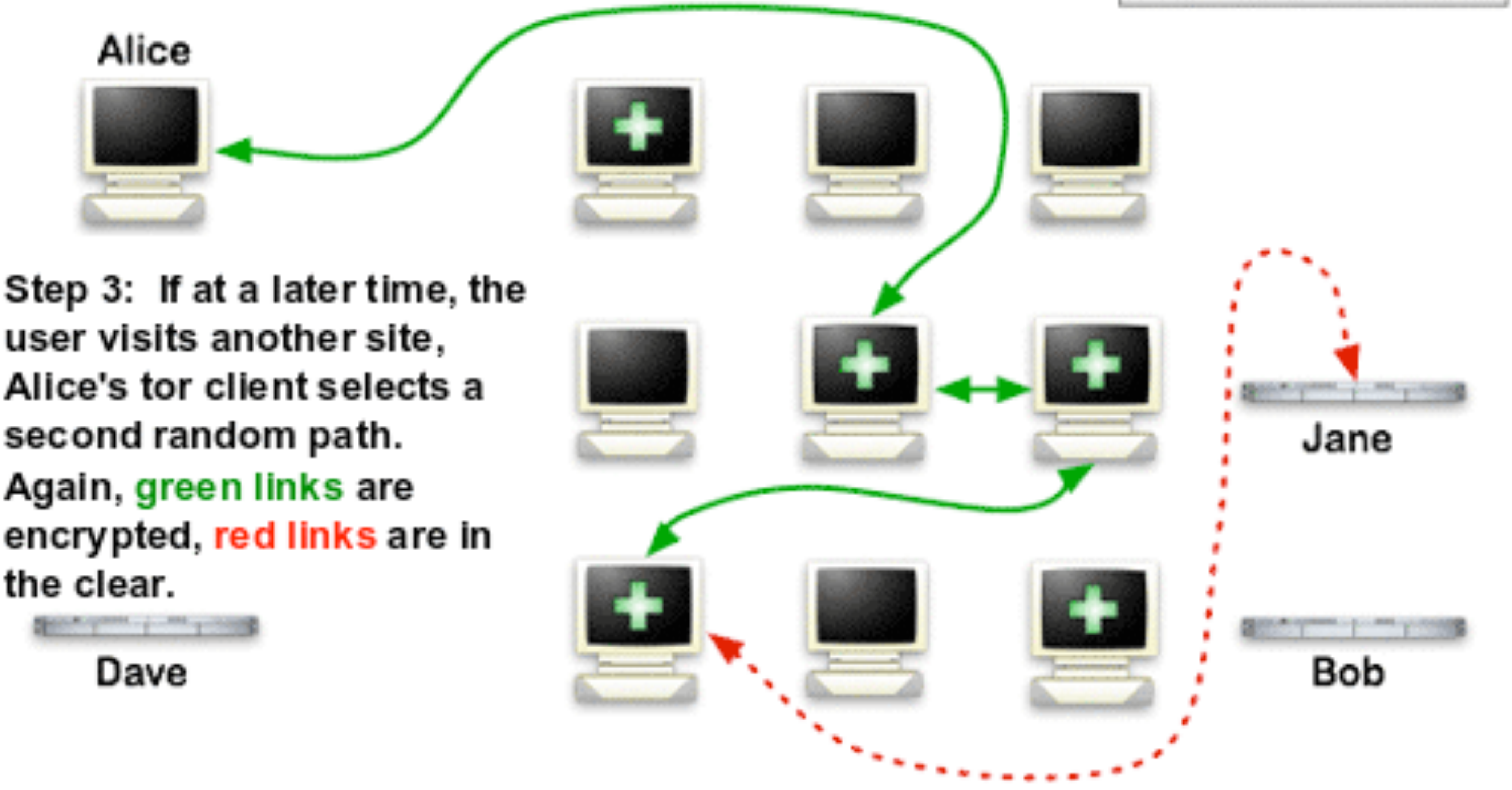


Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

How Tor Works: 3

Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path.

Again, green links are encrypted, red links are in the clear.



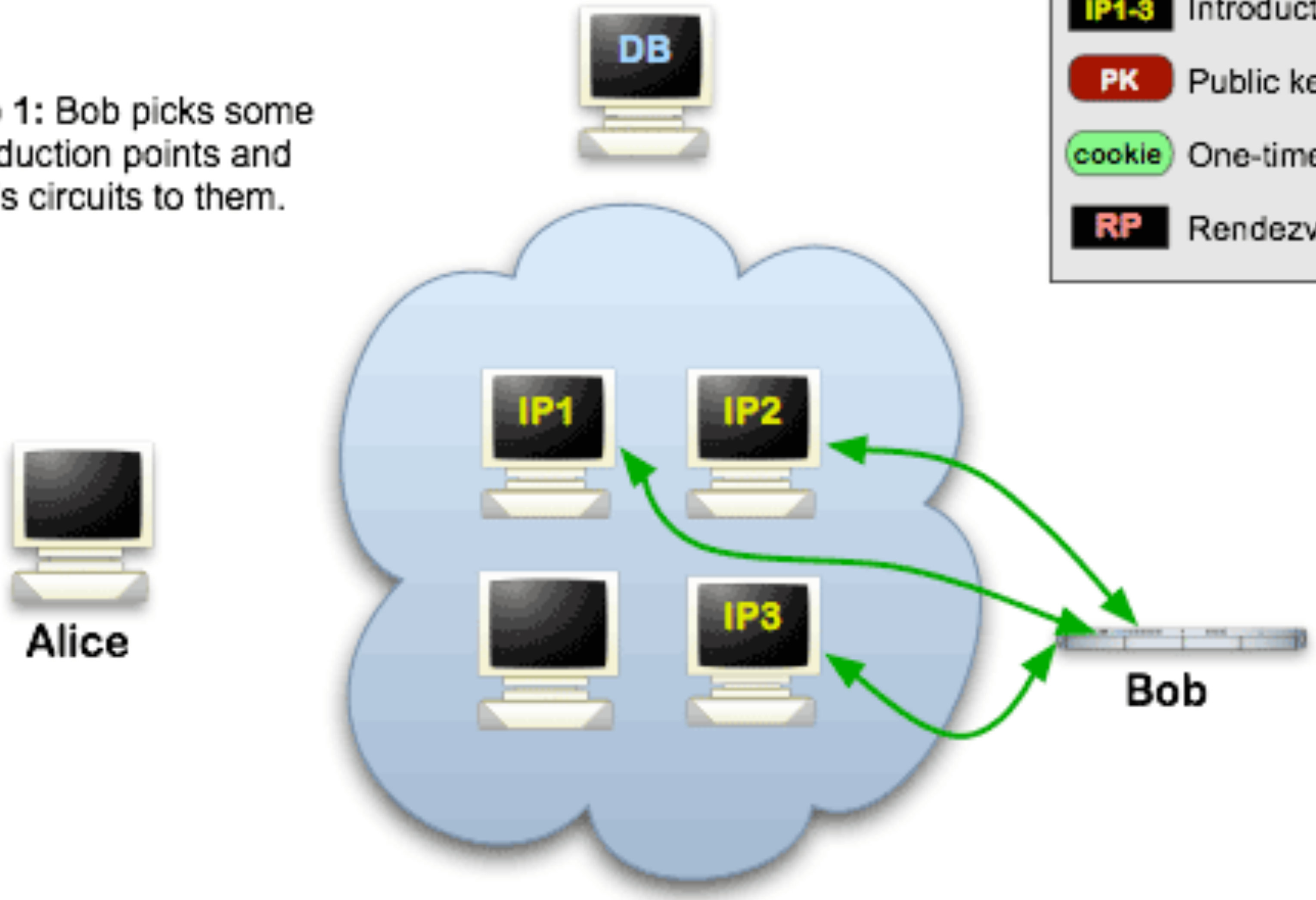
Tor

- Provides anonymity to Internet users
  - No one (except session initiator) knows who is communicating
  - Most common use: Web browsing
- Offers *hidden services*
  - Neither party knows the other’s location
  - Rendezvous via special URL

Onion Services: Step 1

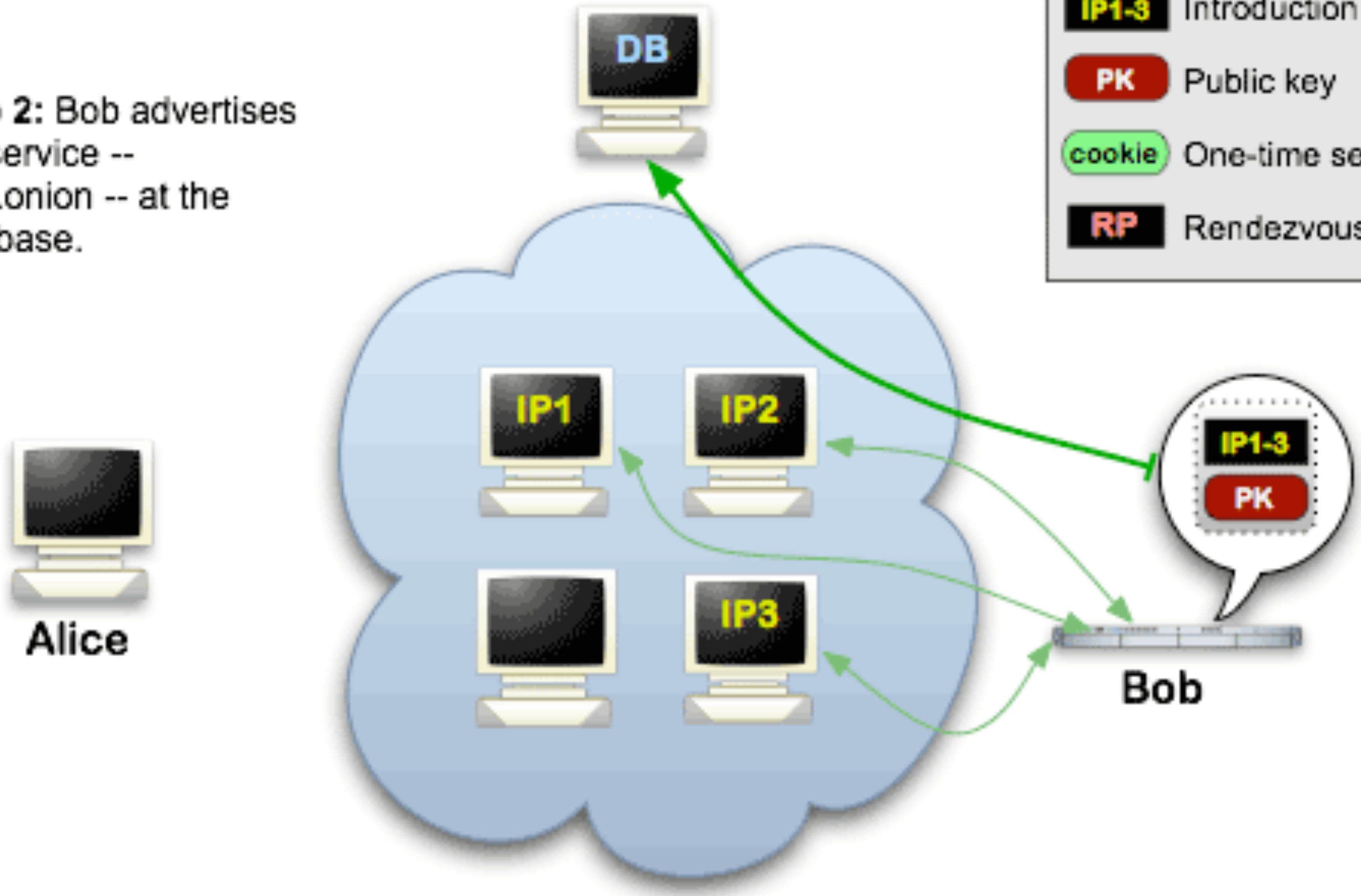
- ☁ Tor cloud
- ⇄ Tor circuit
- IP1-3 Introduction points
- PK Public key
- cookie One-time secret
- RP Rendezvous point

Step 1: Bob picks some introduction points and builds circuits to them.



Onion Services: Step 2

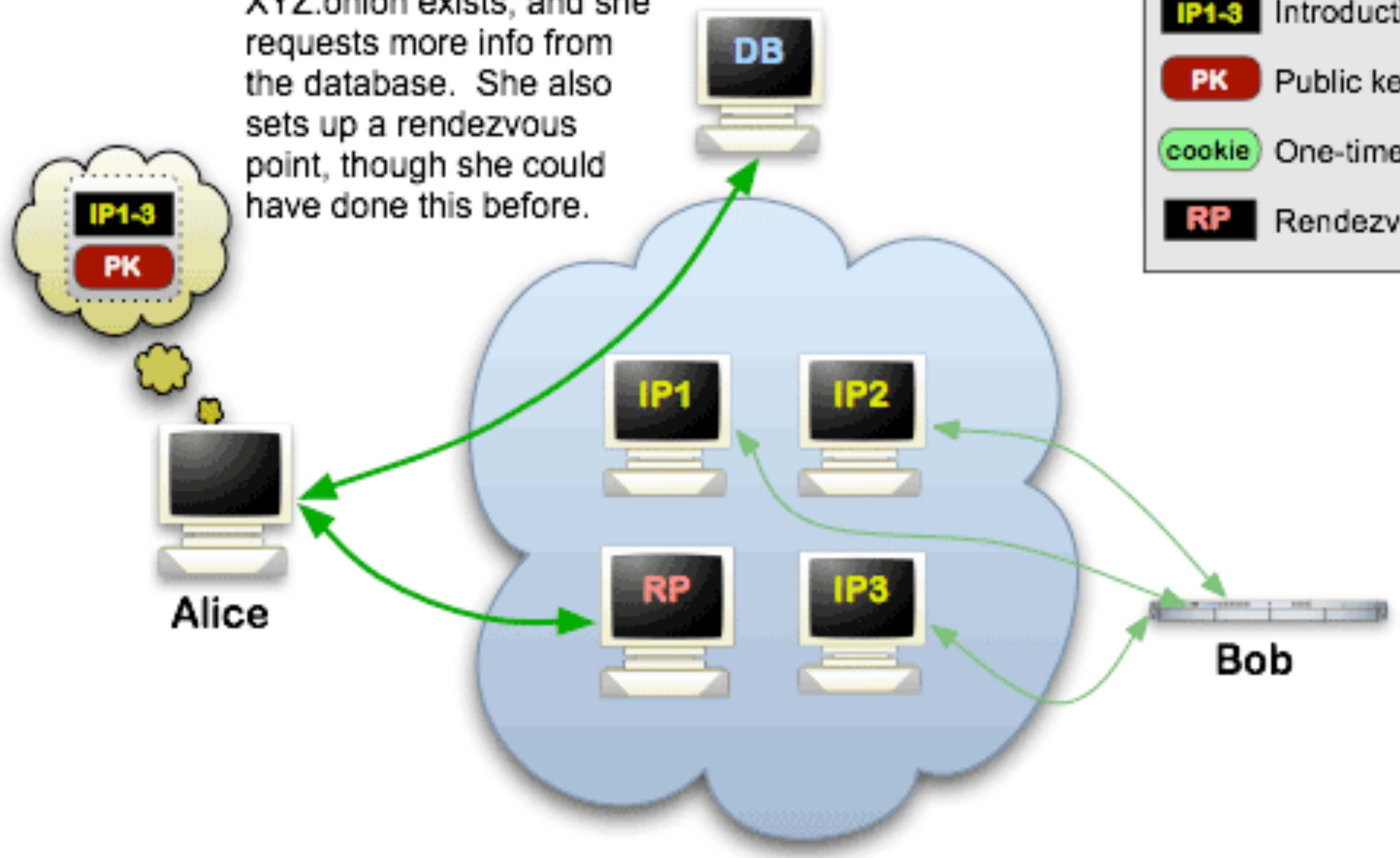
Step 2: Bob advertises his service -- XYZ.onion -- at the database.



- ☁ Tor cloud
- ⟷ Tor circuit
- IP1-3 Introduction points
- PK Public key
- cookie One-time secret
- RP Rendezvous point

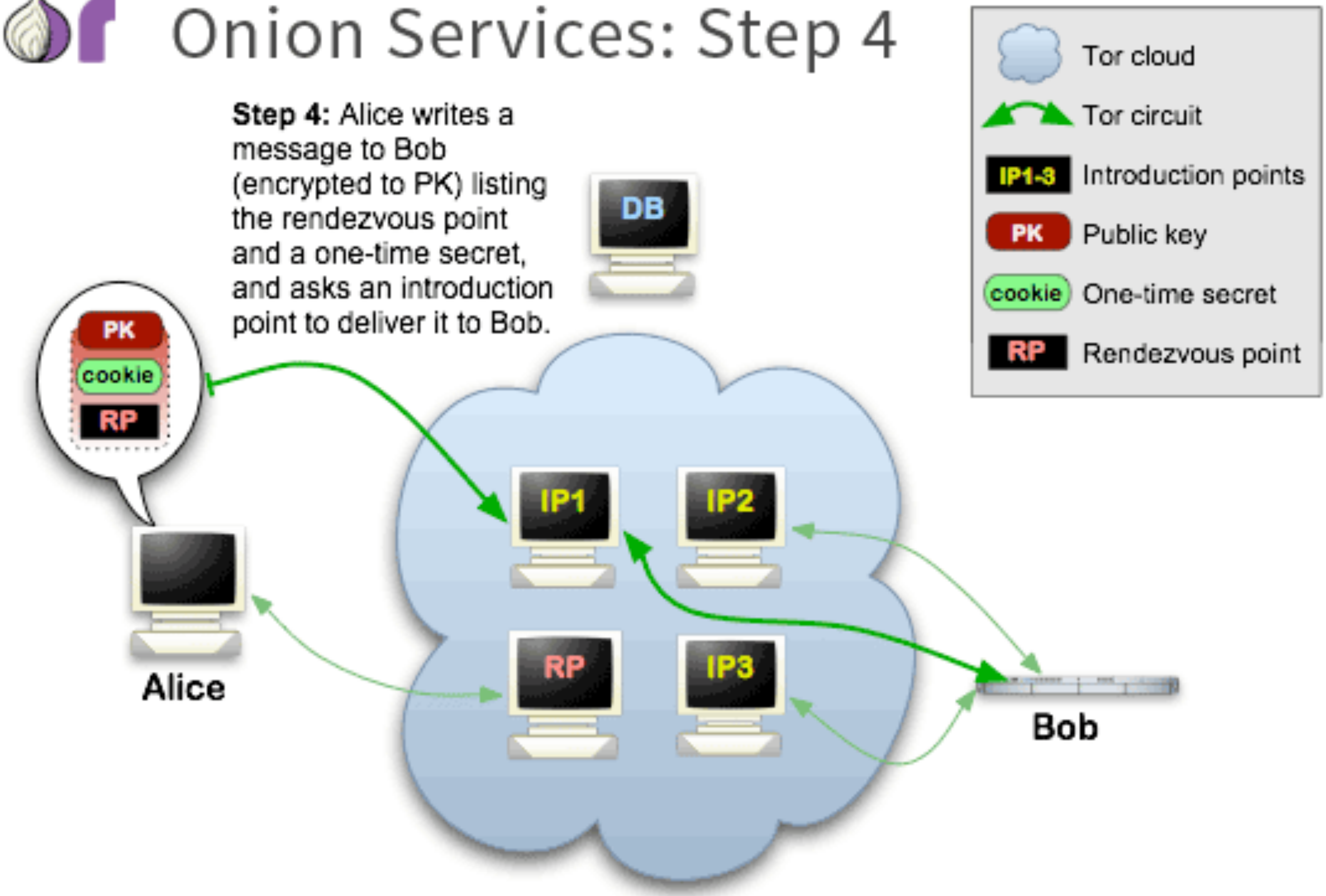
Onion Services: Step 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



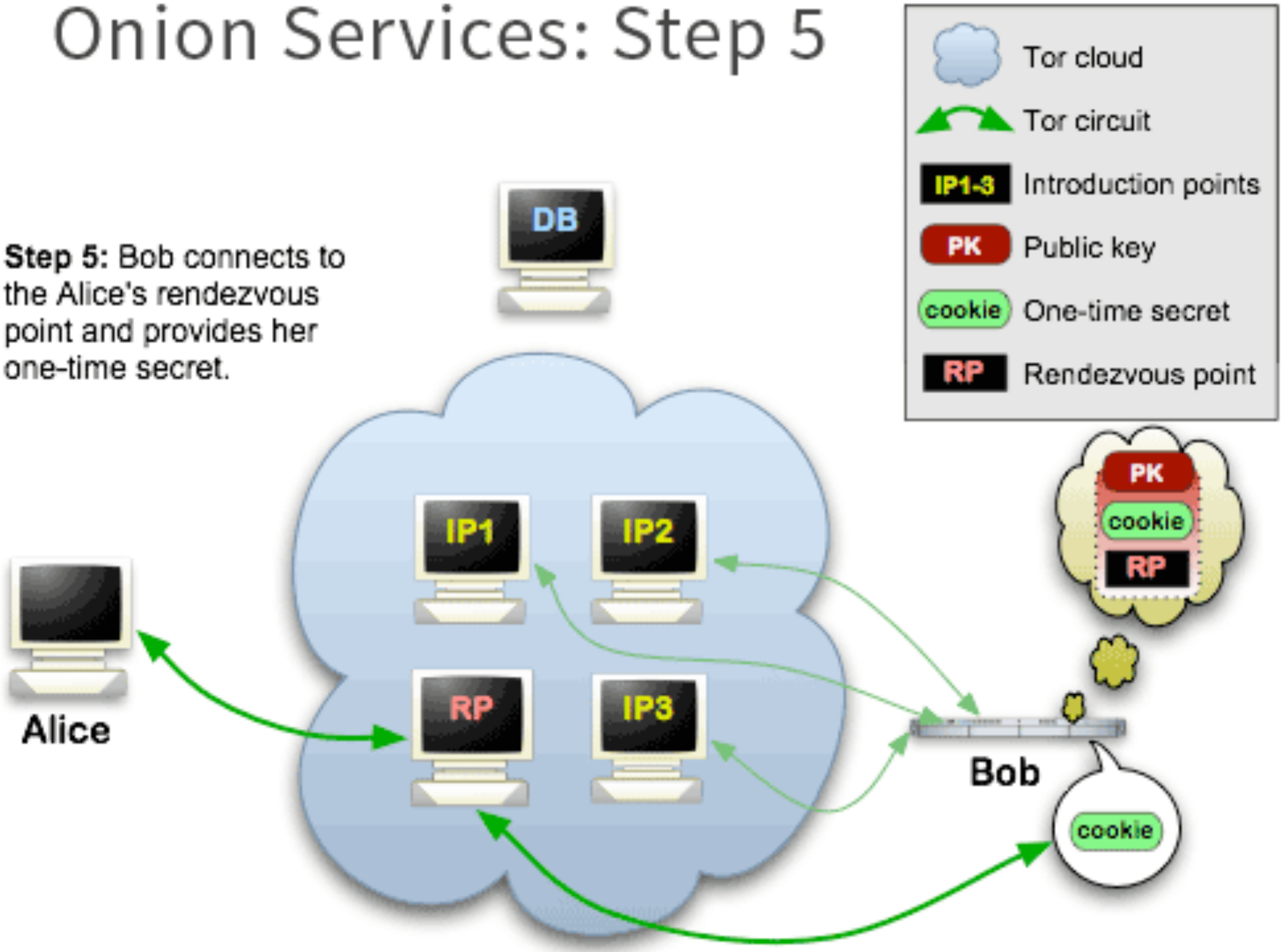
Onion Services: Step 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



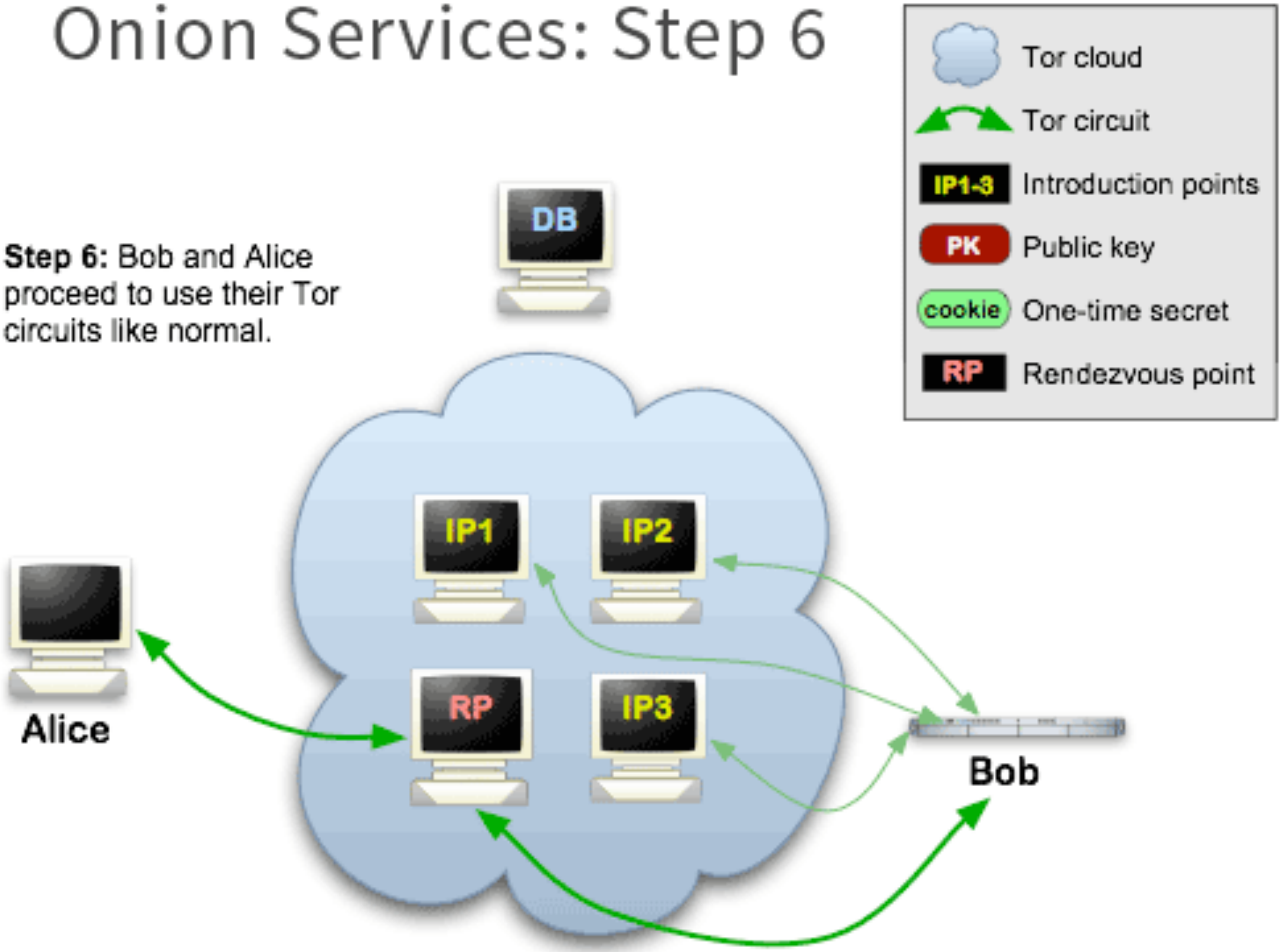
Onion Services: Step 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



Onion Services: Step 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.



Bitcoin

- Most ransomware needs ransom paid in Bitcoin. Why?
  - Presumed anonymity
  - Hard to shut down
- Bitcoin is a public ledger: can see ransom payments
- WannaCry three fixed Bitcoin addresses for ransoms
  - 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
  - 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
  - 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Bitcoin Transactions

- All transactions recorded in shared public ledger
- Bitcoin value associated to a public key **(wallet)**
  - Need private key to spend wallet value
  - Wallet creation is zero cost
- No explicit link to real identities

Bitcoin Transactions

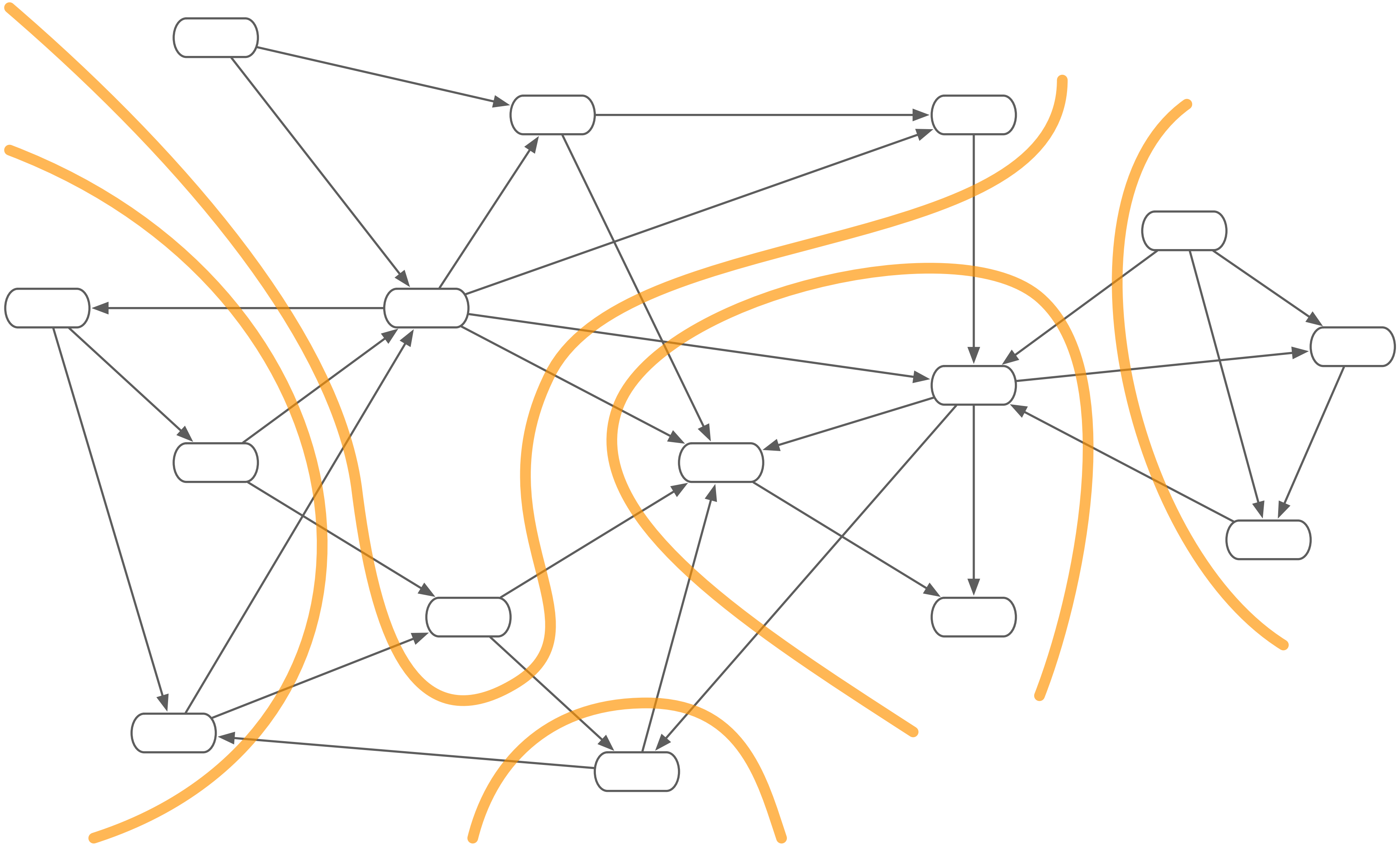
sum of input balances = sum of outputs + fee

- Inputs belong to same person
  - Need wallet private key to spend (use as input)
- Inputs spent completely
- One of the outputs is usually **change** back to sender
  - Change output not marked explicitly

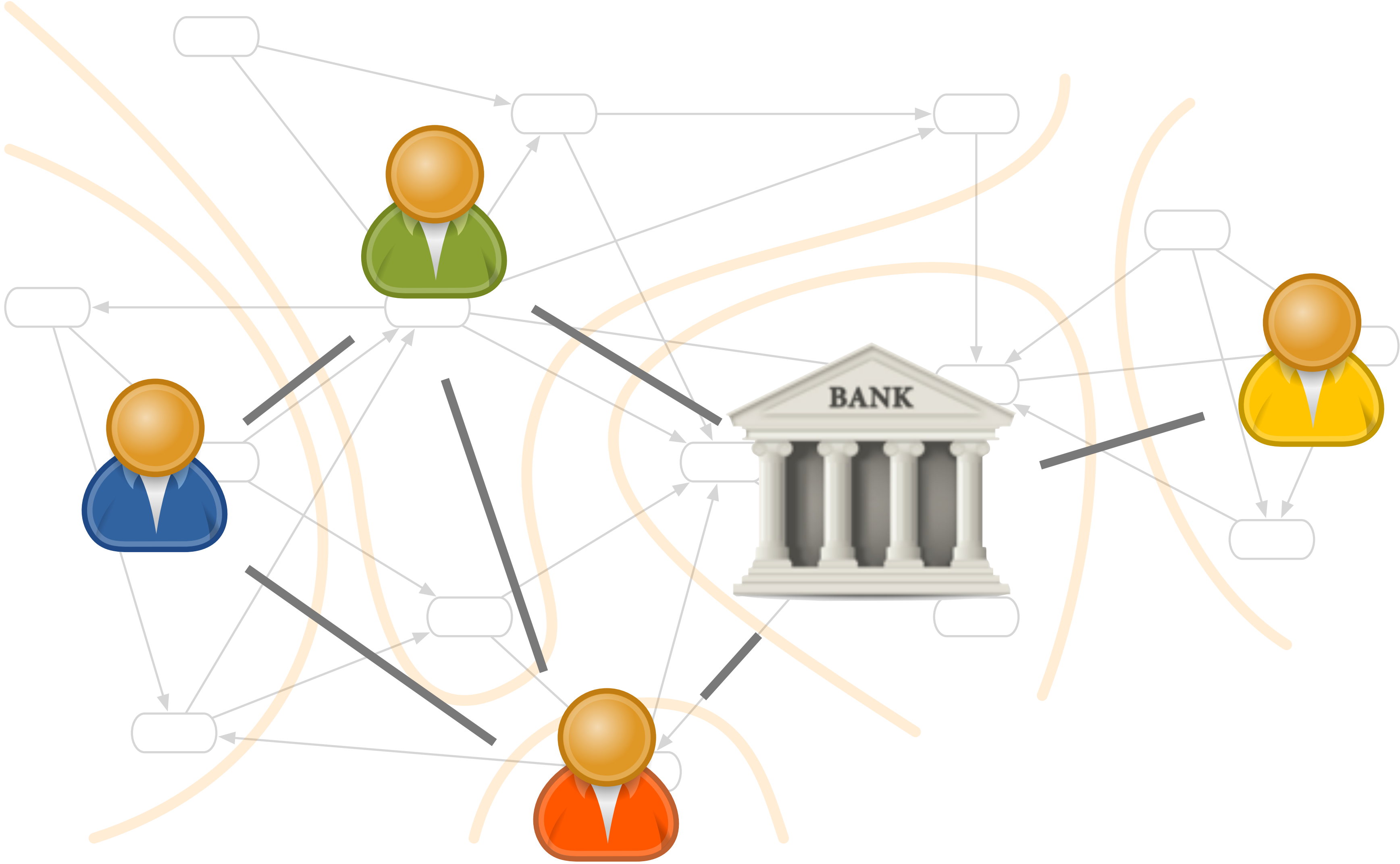
Wallets to Users

- A user has many wallets
  - Zero overhead to create
  - Standard client generates multiple wallets
- Need to group wallets belonging to same user
- Identify major users (exchanges, merchants, etc.)
  - Purchasing goods, public forums

Wallets to Users



Wallets to Users

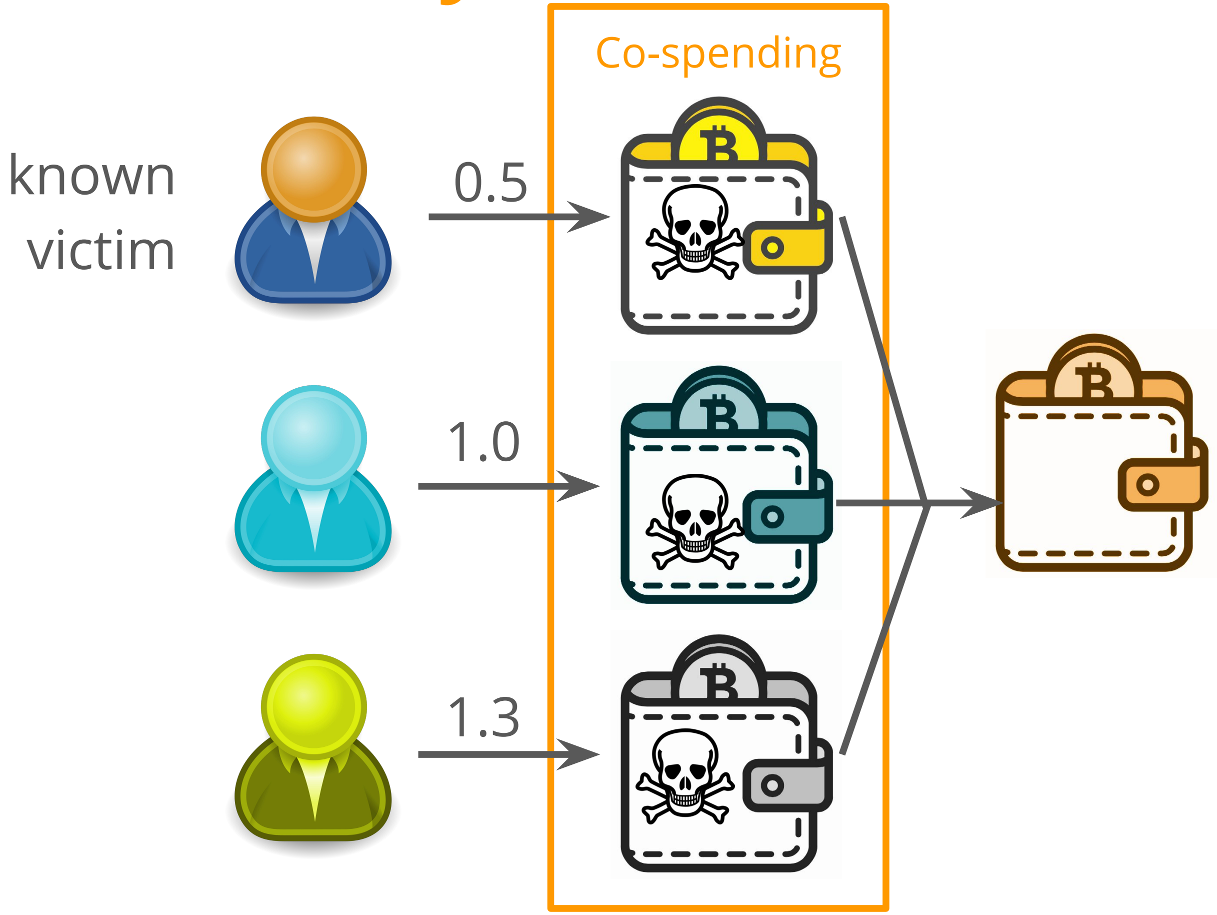


From Wallets to Users

Input rule:
All inputs in a transaction belong to same user.

Methodology: Follow the money

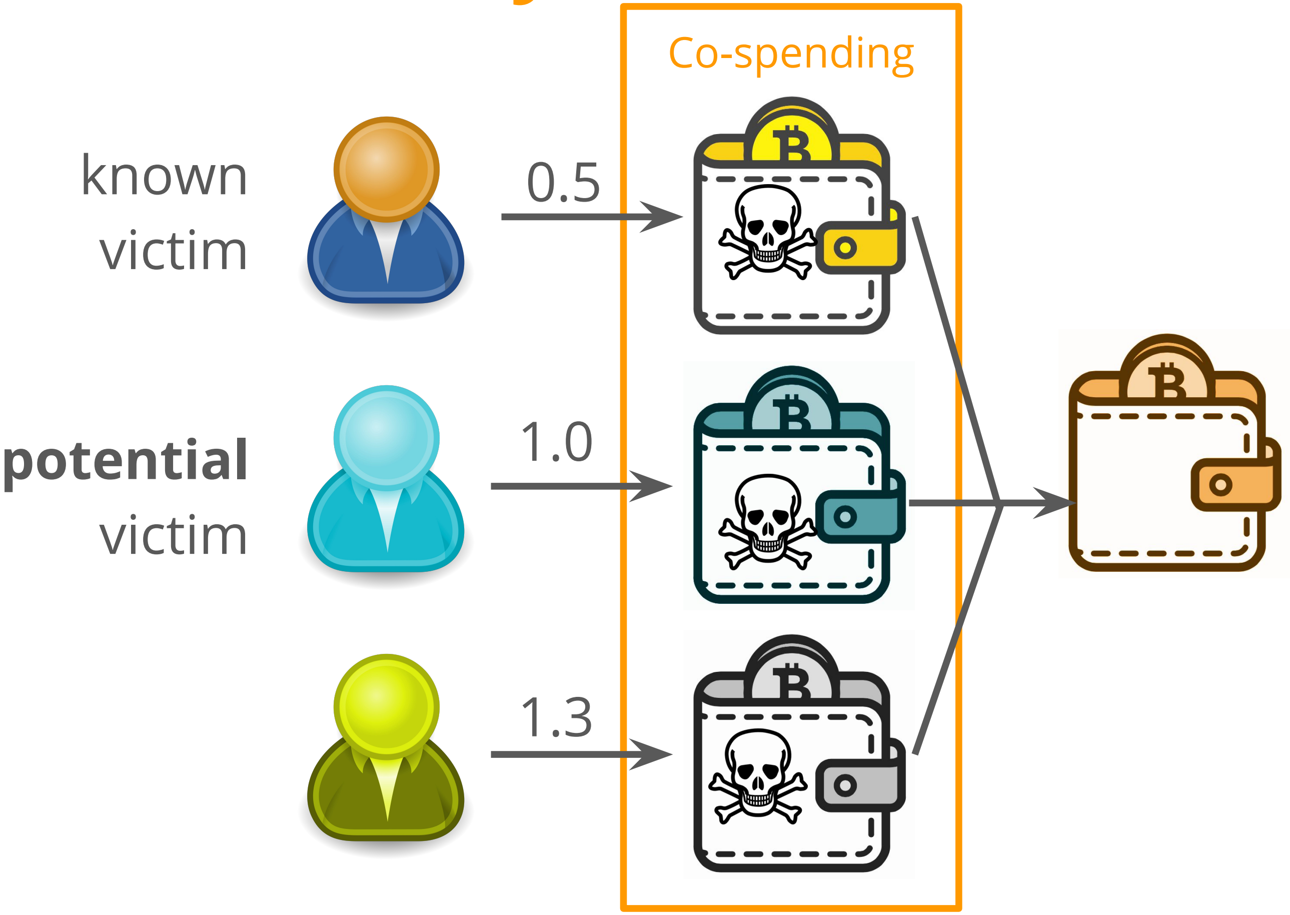
1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom



source: D. Huang *et al.* Tracking Ransomware End-to-End, 2018.

Methodology: Follow the money

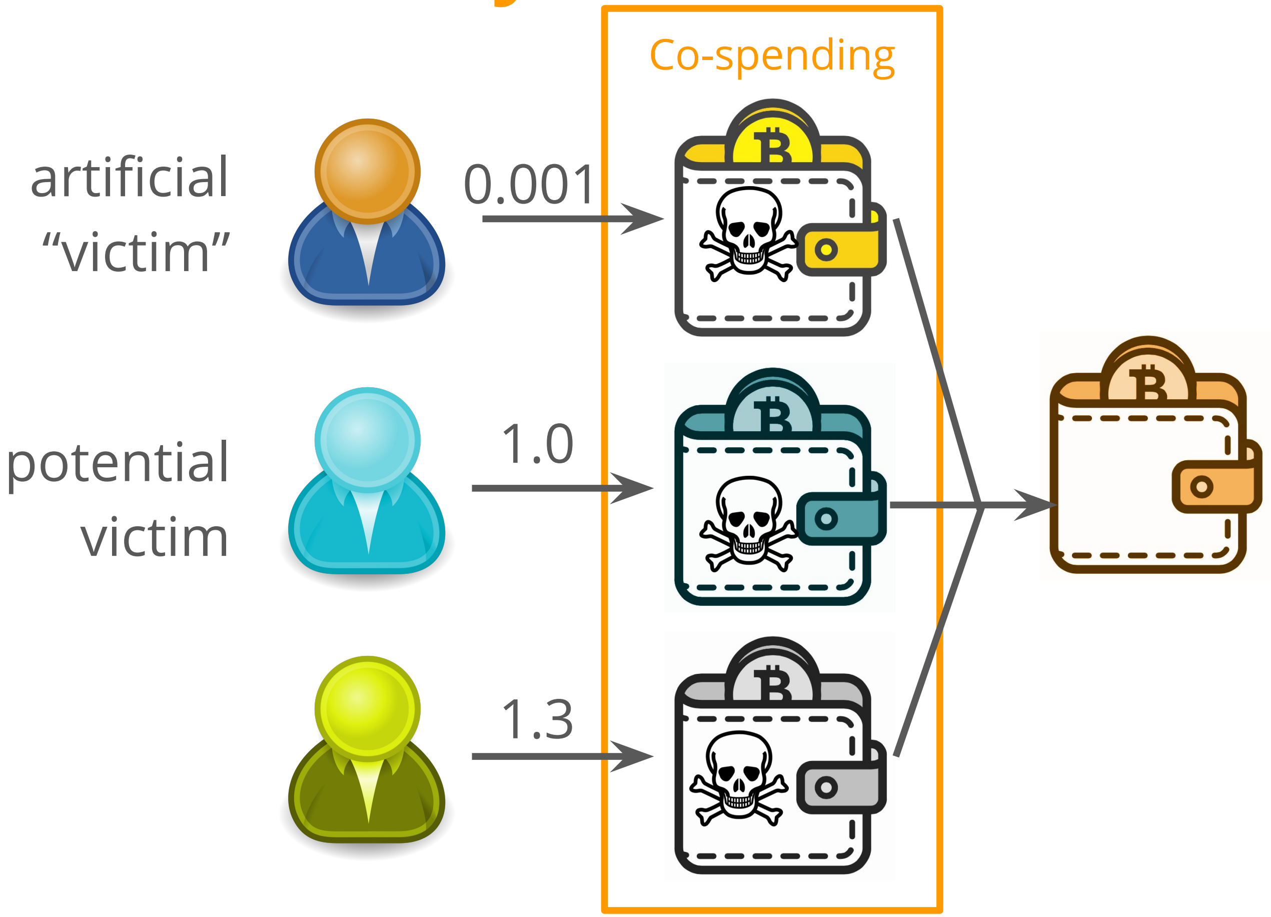
1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom



source: D. Huang *et al.* Tracking Ransomware End-to-End, 2018.

Methodology: Follow the money

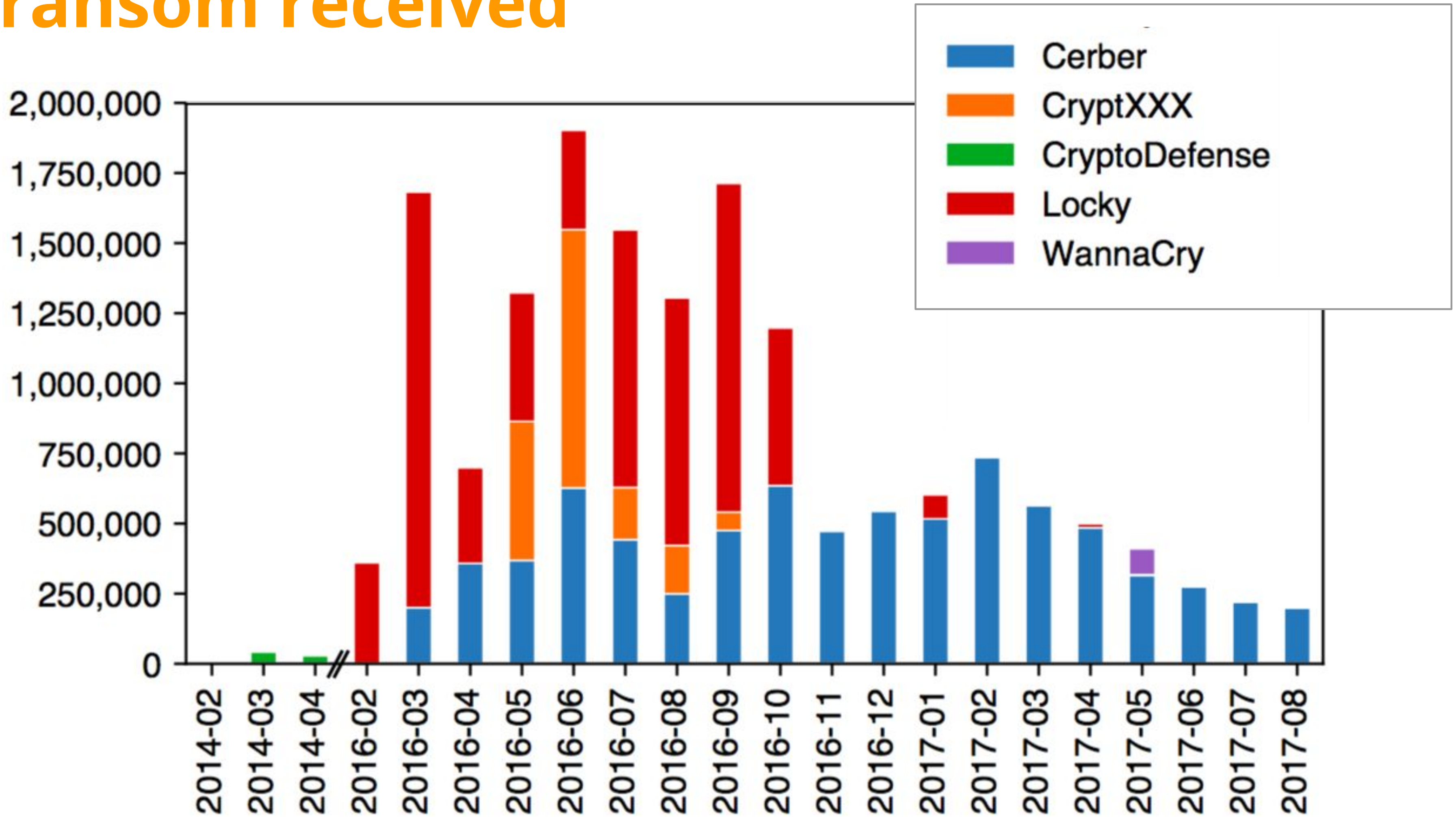
1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom



source: D. Huang *et al.* Tracking Ransomware End-to-End, 2018.

Total ransom received

USD per month



source: D. Huang *et al.* Tracking Ransomware End-to-End, 2018.